REMARKS

The claims remaining in the present application are Claims 1-20. The Examiner is thanked for performing a thorough search. Claims 1, 2, 4, 6-10, and 15-20 have been amended. No new matter has been added. For example, support for the amendments to the highest level Claims 1, 10 and 15 can be found, among other places, at page 18 lines 8-24, original Claim 2, page 20 lines 15-19, page 23 lines 6-13 and Figure 6 of the instant application.

Page 18 lines 8-24 of the instant application state,

> The present invention is capable of prioritizing the functionality provided by components and factoring the prioritization into a security threat indication and response. In one embodiment, a spanning tree representation of a centralized resource network (e.g., server farm, UDC, etc.) is built with asset value and exposure or connectivity indicators that are utilized to determine a risk indicator. The risk indicator indicates the relative threat of disruption of important applications and information supported by a component.

Page 20 lines 15-29 of the instant application state,

> In accordance with one exemplary implementation of the present invention, if an attack attempt penetrates the security measure of component 610, diffusion mitigation actions are applied to component 630, 650 and 690 before components 620, 640 and 670 since components 630, 650 and 690 are on the highest risk path.

Page 23 lines 6-13 of the instant application state,

> Attack spreading response module 720 responds to the risk of an attack spreading to a first component from other components included in the network. The response is performed in accordance with the risk. In one exemplary implementation, possible communication paths are ranked in order of highest risk to lowest risk and the response (e.g., protective mitigation attention) is provided according to the rank. For example, components included in a high ranking communication path... are responded to first...before components with a lower risk value.

The amended dependent claims were amended to provide proper antecedent basis.

CLAIM REJECTIONS

35 U.S.C. §103

Claims 1-9

Claims 1-9 are rejected under 35 U.S.C. §103(a) as being anticipated by U.S. Patent No. 5,850,516 by Schneier et al. (referred to hereinafter as "Schneier") in view of U.S. patent publication no. 2002/0073338 by Burrows et al. (referred to hereinafter as "Burrows"). Applicants respectfully submit that embodiments of the

present invention are neither taught nor suggested by Schneier or Burrows, alone or in combination.

Amended independent Claim 1 recites,

A security intrusion mitigation method comprising:
utilizing network spanning tree configuration information to determine an action for mitigating diffusion of intrusive attacks between components associated with a network, wherein said spanning tree information includes an indication of a first internal diffusion risk and a second internal diffusion risk, wherein said first internal diffusion risk is a risk of a first attack diffusing from a first component associated with said network to a second component associated with said network and said second internal diffusion risk is a risk of a second attack diffusing from a third component associated with said network to said second component;
using said internal diffusion risks to determine that there is a higher risk of said first attack diffusing from said first component to said second component than said second attack diffusing from said third component to said second component; and
using said network spanning tree configuration information to perform said action for mitigating diffusion of intrusive attacks automatically at least in part by mitigating said first attack before mitigating said second attack, wherein said action for mitigating includes compensation for functional support of an application associated with said second component that has priority over another application (emphasis added).

Applicants respectfully submit that Schneier does not teach or suggest, among other things, "wherein said spanning tree information includes an indication of a first internal diffusion risk and a second internal diffusion risk, wherein said first internal diffusion risk is a risk of a first attack diffusing from a first component associated with said network to a second component associated with said network and said second internal diffusion risk is a risk of a second attack diffusing from a third component associated with said network to said second component; using said internal diffusion risks to determine that there is a higher risk of said first attack diffusing from said first component to said second component than said second attack diffusing from said third component to said second component; and using said network spanning tree configuration information to perform said action for mitigating diffusion of intrusive attacks automatically at least in part by mitigating said first attack before mitigating said second attack, wherein said action for mitigating includes compensation for functional support of an application associated with said second component that has priority over another application," (emphasis added) as recited by Claim 1

Schneier teaches a method and apparatus for analyzing information systems using stored tree data structures. For example at Col. 3 lines 10-17, Schneier states,

> The database uses a tree-based structure (an attack tree) to analyze the security of a system. In one embodiment of the invention, the attack tree's root node is the goal of an attacker, the leaf nodes are attacks against the goal, and the intermediate nodes are various combinations of attacks necessary to achieve the goal. Nodes can also include counter measure the system uses to prevent those attacks...

Therefore Schneier's attack tree includes information about the goal of an attacker, attacks against the goal, combinations of attacks to achieve the goal, and possibly counter measures. At Col. 3 lines 31-35, Schneier states, "Applying attack trees to two related systems allows an analyst to compare the two systems, e.g., to show how a specific change to a system affects the overall security of the system, to determine which of several changes to a security system will most increase the overall security of the system..."

Schneier provides specific examples of attack trees at various places such as Col. 7 lines 1-20, Col. 7 lines 52 to Col. 8 line 5, Col. 8 lines 22-43, Col. 9 lines 1-22, Col. 9 lines 31-52, Col. 9 line 65 to Col. 10 line 19, Col. 10 line 31-53, Col. 13 line 10-31, Col. 14 lines 27-49, and Col. 16 lines 20 to Col. 17 line 51 that describe root nodes that are the goals of an attacker, leaf nodes that are attacks, intermediate nodes with various combinations of attacks and some counter measures. For example referring specifically to the attack tree depicted at Col. 16 lines 20 to Col. 17 line 51, Schneier has the root node G8 which states the goal of an attack as "System-wide Attack on the Payment System...," a leaf node G8.1.1.1.1.1.2.1.1 that describes the attack "Find app. Boxes with flawed PRNGs," and a counter measure "Design PRNG properly," and intermediate nodes such as G8.1.1.1.1 or G8.1.1.1.1.1 that describe respectively combinations of attacks such as "Force Message Key Equality," and "Chosen Tag Challenge Attack."

First, Schneier's attack trees do not identify components associated with a network. Second, Schneier's attack trees do not include an indication of a first internal diffusion risk and a second internal diffusion risk, wherein said first internal diffusion risk is a risk of a first attack diffusing from a first component associated with a network to a second component associated with said network and said second internal diffusion risk is a risk of a second attack diffusing from a third component

associated with said network to said second component." Third, since Schneier's attack trees do not include internal diffusion risks, Schneier's cannot teach or suggest, "using said internal diffusion risks to determine that there is a higher risk of said first attack diffusing from said first component to said second component than said second attack diffusing from said third component to said second component." Fourth, Schneier does not use his attack tree to perform actions. Instead Schneier's attack trees are used for comparing the security provided by different systems. Therefore, Schneier cannot teach or suggest, "using said network spanning tree configuration information to perform said action...automatically" (emphasis added). Fifth, Schneier does not teach or suggest "mitigating said first attack before mitigating said second attack" (emphasis added) For example, Schneier does not teach mitigating "Chosen Tag Challenge Attack" associated with intermediate node G8.1.1.1.1.1 before mitigating "Reprogram or Emulate Tags..." associated with intermediate node G8.1.1.1.1.1.1. Sixth, Schneier does not teach prioritizing applications. Therefore Schneier cannot teach or suggest, "wherein said action for mitigating includes compensation for functional support of an application associated with said second component that has priority over another application."

Burrows does not remedy the deficiency in Schneier in that neither Schneier nor Burrows teach or suggest, "wherein said spanning tree information includes an indication of a first internal diffusion risk and a second internal diffusion risk, wherein said first internal diffusion risk is a risk of a first attack diffusing from a first component associated with said network to a second component associated with said network and said second internal diffusion risk is a risk of a second attack diffusing from a third component associated with said network to said second component; using said internal diffusion risks to determine that there is a higher risk of said first attack diffusing from said first component to said second component than said second attack diffusing from said third component to said second component; and using said network spanning tree configuration information to perform said action for mitigating diffusion of intrusive attacks automatically at least in part by mitigating said first attack before mitigating said second attack, wherein said action for mitigating includes compensation for functional support of an application associated with said second component that has priority over another component," (emphasis added) as recited by Claim 1

Referring to the title, Burrows teaches a method and system for limiting the impact of undesirable behavior of computers on a shared data network. Burrows states in the abstract,

> ...The network, through which packets of data are interchanged between the computers, includes one or more forwarding devices that are controlled or instructed by one or more packet traffic monitors. Each of the packet traffic monitors is configured for monitoring the packets; for determining if the information about the pattern of behavior from any of the computers is trustworthy...for determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern behavior; and for determining a proper action for mitigating that type of undesirable behavior.

The Office Action cited paragraphs 0040-0041 of Burrows against the embodiment recited by Claim 1. Burrows states at paragraphs 0040-0041,

> In accordance with its intended purpose, the invention envisions using the packet traffic monitor to determine the existence and source of any pattern of undesirable behavior, including network pathologies such as broadcast storms or ARP fights, and to limit the effects of such behavior. When the packet traffic monitor detects undesirable behavior, including overuse or misuse of the network, as one measure, the monitor takes steps to mitigate this behavior. For example, the packet traffic monitor disables the offending network segment to isolate the offending hosts from the rest of the hosts in the network, or at least from the hosts they are disrupting. Preferably, the invention uses the packet traffic monitor to direct one or more switches (or other forwarding devices such as bridges or smart bridges) to cease forwarding undesirable data traffic.
>
> Thus, upon detecting for example a broadcast storm, the packet traffic monitor mitigates such undesirable behavior patterns by instructing as many switches in the network as possible to stop forwarding those broadcast packets, or perhaps any packets from the offending host. This would allow construction of a large network that would normally allow broadcasts to propagate over the entire network, but which would recover from hosts sending too many broadcast packets. This helps solve a serious problem in conventional networks---especially extended LANs constructed from many Ethernet segments and bridges.

Applicants respectfully agree with the Office Action that Burrows does not teach a "network spanning tree configuration information," as recited by Claim 1. Secondly, Burrows does not teach internal diffusion risks that are risks of an attack diffusing from one component to another component. Third, Burrows does not teach "using said internal diffusion risks to determine that there is a higher risk of said first attack diffusing from said first component to said second component than said second attack diffusing from said third component to said second component." Fourth, Burrows does not teach "using said network spanning tree configuration..."

Fifth, Burrows does not teach "using said network spanning tree configuration to perform said action... by mitigating said first attack before mitigating said second attack..." Sixth, Burrows does not teach prioritizing applications and therefore does not teach or suggest, "wherein said action for mitigating includes compensation for functional support of an application associated with said second component that has priority over another application."

Therefore, independent Claim 1 should be patentable. Claims 2-9 depend on Claim 1. Further, these dependent claims recite additional limitations which further make them patentable. Therefore, these dependent claims should be patentable for at least the reasons that their respective independent claims should be patentable.

For at least the forgoing reasons, Claim 1 should be patentable over Schneier. Claims 2-9 depend on Claim 1 and include all of the features of Claim 1. Therefore these dependent claims should be patentable for at least the reasons that their independent claim should be patentable.

35 U.S.C. §102

Claims 10, 13-17 and 20

Claims 10, 13-17 and 20 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,850,516 by Schneier. Applicants respectfully submit that embodiments of the present invention are neither taught nor suggested by Schneier.

Amended independent Claim 10 recites,

A security intrusion mitigation system comprising:
a means for communicating information;
a means for processing information including instructions for determining a highest risk path that has the highest risk of an attack spreading between network components included in said highest risk path in comparison to risks of attacks spreading between network components associated with other risk paths and automatically mitigating said attack from spreading between said network components included in said highest risk path; and
a means for storing said information, including instructions for storing information describing said highest risk path.

Applicants respectfully submit that Schneier does not teach or suggest, among other things, "determining a highest risk path that has the highest risk of an attack spreading between network components included in said highest risk path in

comparison to risks of attacks spreading between network components associated with other risk paths and automatically mitigating said attack from spreading between said network components included in said highest risk path; and a means for storing said information, including instructions for storing information describing said highest risk path," as recited by Claim 10.

For example, for reasons already discussed herein Schneier does not teach or suggest, determining paths of networked components or determining risks associated with different paths of networked components. Further, Schneier does not teach or suggest using these determined risks as a part of preventing the spread of an attack. Therefore, Schneier cannot teach or suggest "determining a highest risk path that has the highest risk of an attack spreading between network components included in said highest risk path in comparison to risks of attacks spreading between network components associated with other risk paths and automatically mitigating said attack from spreading between said network components included in said highest risk path," nor can Schneier teach or suggest, "a means for storing said information, including instructions for storing information describing said highest risk path."

The Office Action asserts that Schneier teaches the embodiment recited by Claim 10 at Col. 3 lines 15-16, Col. 15 line 37 to Col. 16 line 12, reference number 260 depicted in Figure 2. Col. 3 lines 15-16 state, "It is an object of this invention to determine the vulnerability of a system against attack." Note that Col. 3 lines 15-16 does not teach or suggest, "determining a highest risk path that has the highest risk of an attack spreading between network components included in said highest risk path in comparison to risks of attacks spreading between network components associated with other risk paths and automatically mitigating said attack from spreading between said network components included in said highest risk path; and a means for storing said information, including instructions for storing information describing said highest risk path," as recited by Claim 10.

Col. 15 lines 37 to Col. 16 line 12 provides a description of the attack tree illustrated at Col. 16 lines 20 to Col. 16 line 52. This attack tree does not teach or suggest the embodiment recited by Claim 10 for reasons already discussed herein. The data storage device 260 depicted on Figure 2 does not teach or suggest the embodiment recited by Claim 10 for similar reasons that Schneier's attack tree does

not teach or suggest the embodiment recited by Claim 10. Therefore, independent Claim 10 should be patentable over Schneier. Independent Claim 15 should be patentable over Schneier for similar reasons that independent Claims 1 and 10 should be patentable over Schneier.

Claims 11-14 depend on Claim 10. Claims 16-20 depend on Claim 15. Further, these dependent claims recite additional limitations which further make them patentable. Therefore, these dependent claims should be patentable for at least the reasons that their respective independent claims should be patentable.

CONCLUSION

In light of the above listed amendments and remarks, reconsideration of the rejected claims is requested. Based on the arguments and amendments presented above, it is respectfully submitted that Claims 1-20 overcome the rejections of record. For reasons discussed herein, Applicant respectfully requests that Claims 1-20 be considered be the Examiner. Therefore, allowance of Claims 1-20 is respectfully solicited.

Should the Examiner have a question regarding the instant amendment and response, the Applicant invites the Examiner to contact the Applicant's undersigned representative at the below listed telephone number.

Respectfully submitted,
WAGNER BLECHER LLP

Dated: 9/17, 2007

John P. Wagner Jr.
Registration No. 35,398

Address: Westridge Business Park
123 Westridge Drive
Watsonville, California 95076 USA

Telephone: (408) 377-0500 Voice
(408) 234-3649 Direct/Cell
(831) 722-2350 Facsimile